United States District Court

MIDDLE DISTRICT OF ALABAMA

In the matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

Yahoo!, Inc., 701 First Avenue
Sunnyvale, CA 9408963
Contents of email accounts:
aiaraicubani@yahoo.com
dolarel92@yahoo.com

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 2:06mj4-DRB

I Michael P. Eubanks being duly sworn depose and say:

I am a(n) Federal Bureau of Investigation Special Agent and have reason to believe

that ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

Yahoo!, Inc., 701 First Avenue
Sunnyvale, CA 9408963
Contents of email accounts: aiaraicubani@yahoo.com and dolarel92@yahoo.com

in the Northern District of California

there is now concealed a certain person or property, namely (describe the person or property to be seized)

See Attachment A

which is (state one or more bases for search set forth under Rule 41(b) of the Federal Rules of Criminal Procedure) concerning a violation of Title 18 United States Code, Section(s) 1343 and 2320.

The facts to support the issuance of a Search Warrant are as follows:

See Attached Affidavit Which is Incorporated by Reference Herein

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

Signature of Affiant

Sworn to before me and subscribed in my presence,

December 16, 2005 at Montgomery, Alabama
Date City and State

Delores R. Boyd, U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT

I, MICHAEL P. EUBANKS, being duly sworn depose, say, and provide the following information (obtained by me unless otherwise noted):

I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been assigned to the Mobile, Alabama Division of the FBI since April, 1999. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer fraud and conspiracies to commit those crimes. I have a Master of Science Degree in Software Systems Engineering, a Bachelor of Science Degree in Computer Science, and approximately seven years of professional experience as a computer programmer in private industry. Additionally, I have received special training relevant to the investigation of computer related crimes including courses in network security, advanced computer intrusion investigations, and computer network exploitation.

I am familiar with the information contained in this affidavit from information provided to me in the form of victim and witness interviews, through e-mail correspondence with Colonial Bank information technology and security personnel, by evidence discovered from information returned from Grand Jury subpoenas, discussions with computer experts, and public source information available on the Internet.

This affidavit is offered in support of an application for a search warrant for two e-mail accounts

controlled by the free web-based electronic mail service provider known as Yahoo!, Inc. ("Yahoo!"), headquartered at 701 First Avenue, Sunnyvale, California 94089. The accounts to be searched are **aiaraicubani@yahoo.com** and **dolarel92@yahoo.com**, which are further described in the following paragraphs and in Attachment A. As set forth herein, there is probable cause to believe that on the computer systems of Yahoo!, there exists evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Section 1343, wire fraud and Title 18, United States Code, Section 2320, trafficking in counterfeit goods or services.

In my training and experience, I have learned that Yahoo! is a company that provides free web based Internet electronic mail ("e-mail") access to the general public, and that stored electronic communications, including opened and unopened e-mail for Yahoo! subscribers may be located on the computers of Yahoo!. Further, I am aware that computers at Yahoo! contain information and other stored electronic communications belonging to third parties. Accordingly, this affidavit and application for search warrant seek authorization solely to search the computer accounts and/or files and following the procedures described herein and in Attachment A.

Pursuant to Title 18, United States Code, Section 2703(c)(1)(A), "A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining

to a subscriber to or customer of such service (not including the contents of communications) only when the governmental agency obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation..."

Search Procedure

In order to ensure that agents search only those computer accounts and/or files described herein and in Attachment A, this affidavit and application for search warrant seeks authorization to permit employees of Yahoo! to assist agents executing this warrant to search only those computer accounts and/or files described in Attachment A, the following procedures will be implemented:

1. The search warrant will be presented to Yahoo! personnel who will be directed to isolate those accounts and files described in Attachment A;
2. In order to minimize any disruption of computer service to innocent third parties, Yahoo! employees trained in the operation of computers will create an exact duplicate of the computer accounts and files described below, including an exact duplicate of all information stored in the computer accounts or files described below;
3. Yahoo! personnel will provide the exact

duplicate of the accounts and files described below, and all information stored in those accounts and/or files to the Special Agent who serves this search warrant;

4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from Yahoo! for evidentiary purposes.

Background regarding Computers, the Internet, and E-Mail

The term "computer" as used herein is defined in 18 U.S.C. Section 1030(e)(1), and includes and electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

1. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web ("www") is a functionality of the Internet which allows users of the

Internet to share information;

2. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods;

3. E-Mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer users sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

Yahoo! Mail

Based on my training and experience, I have learned the following about Yahoo! Mail:

1. Yahoo! Mail is an e-mail service which offers e-mail accounts free of charge to Internet users. Subscribers obtain an account by registering on the Internet at the Yahoo! web site (www.yahoo.com). Yahoo! requests

subscribers to provide basic information, such as name, address, zip code, and phone. However, Yahoo! does not verify the information provided;

2. Yahoo! maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information;

3. Subscribers to Yahoo! Mail may access their accounts on servers maintained and/or owned by Yahoo! from any computer connected to the Internet located anywhere in the world;

4. Any e-mail that is sent to a Yahoo! subscriber is stored in the subscriber's "mail box" on Yahoo!'s servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by Yahoo!. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on Yahoo!'s servers indefinitely;

5. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Yahoo!'s servers, and then transmitted to its end destination. Yahoo!

users have the option of saving a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Yahoo! server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained at Yahoo!, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations;

6. A Yahoo! subscriber can store files, including e-mails and image files, on servers maintained and/or owned by Yahoo!;

7. E-mails and image files stored on a Yahoo! server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store e-mails and/or other files on the Yahoo! server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the Yahoo! server.

Probable Cause

This investigation was initiated on July 18, 2005 after security personnel at Colonial Bank contacted the FBI to report a counterfeit Colonial Bank Internet web site created by an unauthorized person(s) which was designed to solicit personal information from bank customers. The solicitation was being conducted by unknown, unauthorized person(s).

Internet "Phishing" Background

The technique utilized by the unauthorized person(s) in this investigation is known as Internet "phishing". "Phishing" is conducted by an unauthorized user who creates an Internet web site which is either a clone of an original Internet web site or else is a customized web site which utilizes counterfeit marks in an effort to appear as if it a site which belongs to the company or organization being targeted in the scheme. After the creation of the web site, the perpetrator conducts an unlawful computer intrusion and obtains access to a computer system on which the counterfeit web site can be hosted for viewing by all Internet users. Once the web site is running on the victim computer system, the perpetrator uses a variety of techniques to make the website appear authentic, including creating a web site name which closely resembles that of the authentic site. Potential users of the authentic website are

then identified through targeted e-mail "harvesting" from the Internet. Mass e-mail solicitation is then performed in an effort to direct these potential victims to the cloned web site where they are requested to provide specific financial information. Once obtained by the perpetrators, this financial information is then abused for their own financial gain.

The victims in Internet "phishing" schemes include the targeted corporation for which the counterfeit web site created, the targeted recipients of the mass e-mail solicitations whom respond to the "phishing" e-mail, and the corporation or person whose computer was used to host the counterfeit web site.

Losses in phishing schemes can be quantified through the time devoted by Information Technology personnel responding to each "phishing" attack. Response includes time devoted by personnel in negotiating the removal of the web site from the Internet and costs to the bank for contracting experts in the removal of such sites. This does not include the loss to the solicited victims of each "phish" or to the victim company where the intruder hosted the "phishing" web site. Evidence from computers on which the counterfeit "phishing" web site was hosted is difficult to obtain since these computers are often located throughout the world and are only active for short periods of time.

"Phishing" Incident on July 18, 2005

On July 18, 2005, Colonial Bank Information

Technology personnel were notified by a bank customer that they had received an e-mail referring them to a web site which appeared to be suspicious. According to the customer, the e-mail advised that Colonial Bank was conducting a security verification and the recipients were requested to electronically provide the following information for their Colonial Bank accounts: Username, password, credit card number, Personal Identification Number (PIN), CVV number for the credit card, card expiration date, and e-mail address. CVV stands for 'card verification value'. The CVV number is a three or four digit authentication code on a credit card in addition to the card number. It is used as an anti-fraud security feature that a merchant would ask for to help verify that the cardholder actually has possession of the credit card.

Colonial Bank Information Security Personnel conducted online research to find the source of the web site. It was determined to be located on a server computer of a software development company named Internetwork Publishing Corporation (IPC), 5455 North Federal Highway, Suite O, Boca Raton, Florida. The company was then notified by Colonial Bank personnel that the counterfeit web site was hosted on their computers. The system administrator at IPC reviewed their computer system log files and advised Colonial Bank officials that IPC had been the victim of a computer intrusion. The administrator at IPC e-mailed CHAD SMITH, an information security specialist at Colonial Bank, copies of the electronic files for the counterfeit web site. The IPC

administrator then removed the hard disk drive containing the "phishing" web site and provided it to the Colonial Bank Information Security Department personnel, who then created a forensic image of the disk drive for evidentiary purposes.

Colonial Bank employee CHAD SMITH contacted the FBI Office in Mobile, Alabama on July 18, 2005 regarding the incident. SMITH provided images containing screen captures of the counterfeit web site to the FBI and details regarding IPC's cooperation in the incident.

On November 16, 2005, SMITH provided the FBI with the electronic web site files from the IPC server computers and they were reviewed for further evidence. Two e-mail addresses were discovered which are the destination addresses for all financial information entered by the potential victims. The address were listed in the "phishing" data files were **dolarel92@yahoo.com** and **aiaraicubani@yahoo.com**.

Conclusion

Based on the information above, your affiant believes that on the computer systems owned, maintained, and/or operated by Yahoo!, Inc., headquartered at 701 First Avenue, Sunnyvale, California 94089, there exists evidence, fruits, and instrumentalities of violations of Title 18, U.S.C., Section 1343 and Title 18, U.S.C. Section 2320. By this affidavit and application, I request that the Court issue a search warrant directed at Yahoo! allowing agents to seize the e-mail and other information stored on the Yahoo!

servers for the computer accounts and files and following the search procedure described in Attachment A.

Michael P. Eubanks
Special Agent
Federal Bureau of Investigation
Mobile, Alabama

Subscribed and sworn to before me this 16th day of December, 2005

Delores R. Boyd
U.S. Magistrate Judge

Attachment A

A. Search Procedure

In order to ensure that agents search only those computer accounts or computer files described in Attachment A, this search warrant seeks authorization to permit employees of Yahoo!, Inc. to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts or computer files described in Attachment A, the following procedures have been implemented:

1. The warrant will be presented to Yahoo! personnel who will be directed to isolate those accounts and files described in Attachment A;

2. In order to minimize any disruption of computer service to innocent third parties, the systems administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts or files described in Attachment A;

3. Yahoo! personnel will provide the exact duplicate of the accounts and files described in Attachment A and all information stored in those accounts and/or files to the Special Agent who serves this search warrant;

4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from Yahoo! and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant;

5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the systems administrator and will not further review the original duplicate absent an order of the Court; and

B. Description of Accounts and Computer Files to be Copied by Yahoo!, Inc.

All electronic mail stored and presently contained in, or on behalf of, the following email addresses or individual accounts: **aiaraicubani@yahoo.com and dolarel92@yahoo.com.**

1. Printouts of all of the above from original storage.

2. Any and all transactional information, to include log files, of all activity to the above-listed individuals which includes dates, time, method of connecting, port, dial-up, and/or location, including source IP address(es) and destination IP address(es) of any and all e-mails sent or received by the Yahoo! account names

aiaraicubani@yahoo.com and dolarel92@yahoo.com.

3. All business records and subscriber information, in any form kept, which pertain to the above listed subscribers and accounts, including but not limited to applications, subscribers' full names, all screen names associated with those subscribers and accounts, all account names associated with those subscribers, method of payment, phone numbers, addresses, and detailed-billing records.

C. Description of Information to be Further Copied by Law Enforcement Personnel

1. All communications within the email accounts of **aiaraicubani@yahoo.com and dolarel92@yahoo.com.** that:

   a. are to or from or refer to the email account **aiaraicubani@yahoo.com and dolarel92@yahoo.com.**.

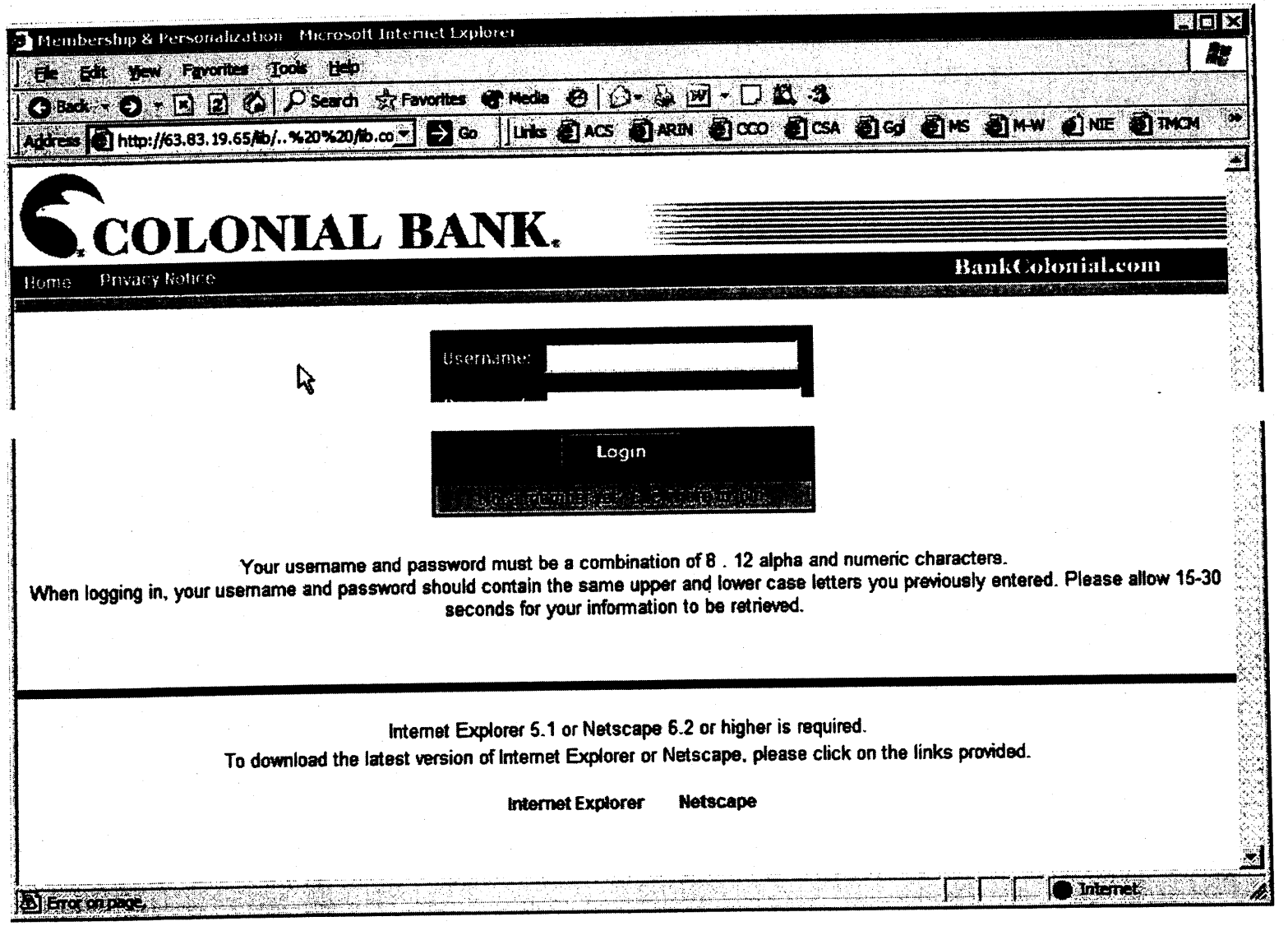
   b. refer to interstate or international travel.

2. All items identified in section B, paragraph 2, of this attachment that relate to those communications identified as being described in section C, paragraphs 1 and 2, of this Attachment.

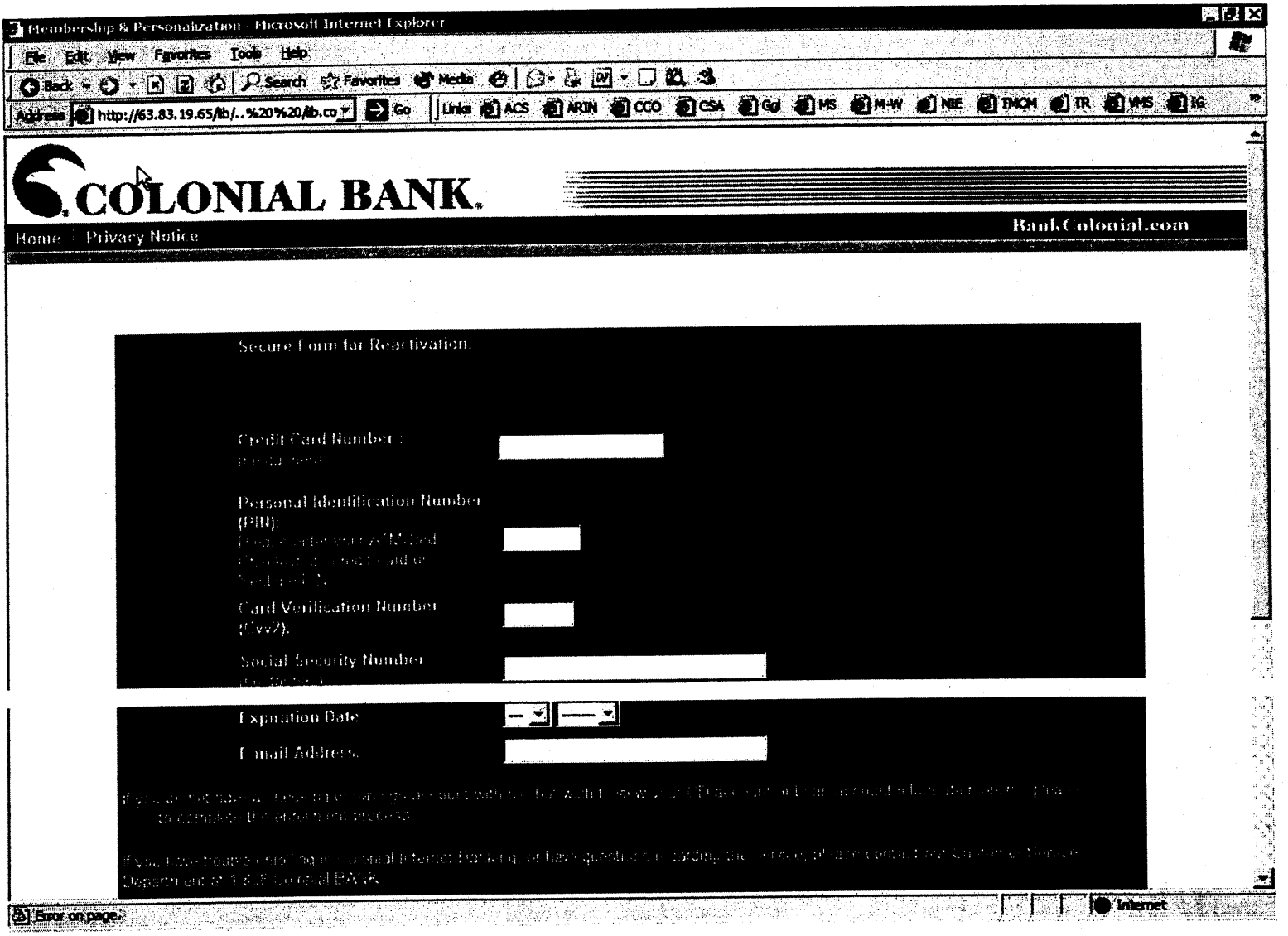
3. All items identified in section B, paragraph 3, of this Attachment.

Any communications or files which can be provided in electronic format (ie: CD) would be preferable, if at all possible.

END OF ATTACHMENT



ATTACHMENT B


Membership & Personalization - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://63.83.19.65/ib/..%20%20/ib.co
Go
Links ACS ARIN CCO CSA Gd MS M-W NBE TMCM TR WMS IG
COLONIAL BANK.
Home Privacy Notice
BankColonial.com
Secure Form for Reactivation.
Credit Card Number :
Personal Identification Number (PIN):
Card Verification Number (Cvv2):
Social Security Number
Expiration Date
E-mail Address:
Error on page.
Internet